Article:

Du, M., Zhang, J. orcid.org/0000-0002-6188-4108, Gu, C. orcid.org/0000-0002-3306-767X et al. (1 more author) (2024) Resilience improving strategy for power systems with high wind power penetration against uncertain attacks. IEEE Transactions on Sustainable Energy, 15 (4). pp. 2625-2637. ISSN 1949-3029

https://doi.org/10.1109/tste.2024.3430844

Resilience Improving Strategy for Power Systems With High Wind Power Penetration Against Uncertain Attacks

Min Du, *Member, IEEE*, Jinning Zhang, Chenghong Gu, *Member, IEEE*, Xin Zhang, *Senior Member, IEEE*

***Abstract*— This paper aims to produce a practical and efficient decision for the system operator to harden critical components in power systems with high wind power penetration against uncertain attacks. Thus, an adjustable robust tri-level defender-attacker-defender (ART-DAD) model is proposed to improve the resilience of power systems by hardening critical transmission lines. The proposed ART-DAD model considers both uncertain attacks and uncertain wind power output, which provides meaningful insights into the resilience improvement of power systems that involve uncertainties. More specifically, the proposed defense model integrates dynamic N-K criterion for attack budgets and the polyhedral uncertainty set for wind power output to develop resilient line hardening strategies. The proposed defense model can be formulated as a mixed integer tri-level programming problem that is decoupled into a master and sub-problem. Then, a constraint-generation based solution algorithm is proposed to solve the overall ART-DAD model with a master and sub-problem scheme. Simulation results on IEEE RTS-79 and RTS-96 systems validate the effectiveness of the proposed resilience improving strategy.**

***Index Terms*— Line hardening, adjustable robust model, defender-attacker-defender, power systems, uncertain attacks, wind power.**

NOMENCLATURE

Sets

$\boldsymbol{B}$	Set of buses.
$\boldsymbol{D}$	Set of loads.
$\boldsymbol{G}$	Set of units.
$\boldsymbol{L}$	Set of lines.
$\boldsymbol{W}$	Set of wind farms (WFs).
$\boldsymbol{S}$	Attack budget scenario set.

Indices and Parameters

b	Index for system buses.
d	Index for loads.
i	Index for units.
l	Index for lines.
w	Index for WFs.
X_l	Reactance of line l.
NW	Total number of WFs.
Π	The uncertainty budget.
R_{L}	The defense resource of the defender.
$R_{\mathrm{A}}(s)$	The specific attack budget in attack budget scenario s.
$\Omega(s)$	Probability of attack budget scenario s.
$P_{\mathrm{G}i}^{\max}$	Maximum power output of unit i.
$P_{\mathrm{D}d}^{\max}$	Maximum power consumed of load d.
$P_{\mathrm{F}l}^{\max}$	Power flow capacity of line l.
$\theta_b^{\max}$	Maximum phase angle at bus b.
$\overline{P}_{\mathrm{W},w}$	Forecasted wind power output of WF w.
$\Delta P_{\mathrm{W},w}$	Maximum wind power output variation of WF w.
$C_{\mathrm{L}l}$	Marginal cost of hardening line l.
$C_{\mathrm{G}i}$	Marginal cost of generation dispatch by unit i.
$C_{\mathrm{D}d}$	Marginal cost of load shedding by load d.

Variables

d_l	Binary variable equal to 1 if line l is defended and hardened, or 0 otherwise.
$a_l(s)$	Binary variable equal to 0 if line l is attacked, or 1 otherwise in attack budget scenario s.
$P_{\mathrm{G}i}(s)$	Power output of unit i in attack budget scenario s.
$P_{\mathrm{W}w}(s)$	Power output of WF w in attack budget scenario s.
$\Delta P_{\mathrm{D}d}(s)$	Load shedding of load d in attack budget scenario s.
$P_{\mathrm{F}l}(s)$	Power flow of line l in attack budget scenario s.
$\theta_b(s)$	Phase angle at bus b in attack budget scenario s.

This work was supported in part by the UK Research and Innovation Future Leaders Fellowship entitled 'Digitalisation of Electrical Power and Energy Systems Operation' under Grant MR/W011360/2. (*Corresponding author: Xin* Zhang.)

M. Du and X. Zhang are with the School of Electrical and Electronic Engineering, University of Sheffield, Sheffield, S10 2TN United Kingdom (e-mail: m.du@sheffield.ac.uk; xin.zhang1@sheffield.ac.uk).

J. Zhang is with School of Engineering, University of Leicester, Leicester, LE1 7RH United Kingdom (e-mail: jz388@leicester.ac.uk).

C. Gu is with the Department of Electronic and Electrical Engineering, University of Bath, Bath, BA2 7AY United Kingdom. (e-mail: C.Gu@bath.ac.uk)

I. INTRODUCTION

In recent years, practical cases of attacks including human attacks and natural disaster attacks on power systems have been reported [1-3]. For example, in January 2015, attackers launched a physical attack on the transmission lines in Pakistan, which resulted in a nationwide power outage and affected 140 million people for several hours [4]. In December 2015, Ukraine power system was attacked and the cyber attacker remotely disabled critical infrastructure components, including switches and circuit breakers, causing widespread power outages across multiple regions of Ukraine [5]. In October 2015, Zhanjiang city in China was attacked by a hurricane named "rainbow" that resulted in a 4.24 million kWh energy shortage [6]. In November 2023, a severe storm with coastal flooding in the Black Sea region destroyed transmission lines and left over half a million people without electricity in southern Russia and Ukraine [7]. Therefore, it is important to improve the resilience strategy in order to mitigate the effects of attacks on power systems.

Researchers have investigated defense strategies to improve the resilience of power systems against attacks [8]. Resilience of power systems is defined as the ability to resist, adapt to, and quickly recover from attacks [9]. At present, line hardening is regarded as an effective measure to improve the resilience of power systems, since it can help the defender to protect critical assets and alleviate the effects of potential attacks on power systems. Therefore, the authors in [10] proposed an attacker-defender (AD) model to formulate defense decisions against attacks based on N-K criterion. However, the authors in [11] pointed out that the AD model was only effective on obtaining near-optimal line hardening strategy. This AD model only considered the bi-level problem to passively defend attacks, without the formulation of pre-defense strategy in response to attacks. Then, the authors in [12] extended the AD model into a tri-level attacker-defender-attacker (DAD) model to determine the optimal line hardening strategy. In [13], the authors proposed a coordinated planning method to harden the lines for improving the resilience of a power system against attacks. In [4], a tri-level defense method was proposed to allocate limited defense resources to improve the resilience of power systems against attacks. In addition, the authors in [14] developed the network topology optimization model to improve the resilience of power systems against attacks. Although the previous research work claimed to improve the resilience of power systems, the impacts of renewable energy uncertainty on power system resilience and defense strategy were previously ignored.

Besides the attacks on power systems, large shares of renewable energy, such as wind power, may impose significant disruption on power systems due to its intermittent nature. With the increasing penetration of wind power into power systems globally, countries such as Denmark has reached 48% of the electricity generated by wind energy [15]. Due to the wind power output uncertainty, wind turbines are vulnerable to attacks which could be hidden from the wind power uncertainty to avoid detection. The authors in [16] revealed that an attacker can launch false data injection attacks on rotor speed values, which increased the fluctuation of wind power output, reduced power generation efficiency, and resulted in the equipment damage. Meanwhile, an adaptive resilient control method was proposed in [16] to improve the resilience of power systems against false data injection attacks on variable-speed wind turbines. The authors in [17] developed a dual-triggered adaptive torque control strategy for power systems against denial-of-service attacks. Such attacks on the variable-speed wind turbines reduced the wind power generation and introduced the errors between the actual and the expected wind power output. Time-delay attacks on the rotor speed sensor measurement of wind turbines could cause large variation of wind power output, and an adaptive observer-based resilient control strategy was proposed in [18] to improve the resilience of power systems against time-delay attacks. In practice, the corrupted wind power outputs in [16-18] were controlled by attackers to deliberately not exceed the maximum deviation of the expected wind power output. Such attacks on wind turbines usually controlled the wind power output within the certain range of fluctuations to avoid detection. In addition, these control mitigation strategies on wind turbine attacks in [16-18] ignored the impact of wind power output's inherent uncertainty on power systems.

Accordingly, system operator is responsible for dealing with the uncertainty of wind power and improving the resilience strategies of power systems against attacks. Then, the authors in [19] proposed a data-driven distributionally robust optimization model to deal with the wind power uncertainty in order to improve the resilience of power systems against attacks. However, this defense model required massive discrete scenarios to cover certain critical scenarios that compromised the power system performance. The increase in the number of discrete scenarios and iterative solutions greatly affected the solution speed of the distributionally robust defense model, and even caused the intractable optimization problem. Thus, the authors in [20] developed a robust line hardening method against the worst N-K contingencies in distribution systems with various renewable energy resources. Specifically, this defense model captured the wind power output uncertainty based on the stochastic programming approach. This approach usually required a priori probability distribution function to characterize the uncertainty realization, which relied on massive detailed historical information of the random variables. Meanwhile, massive random scenarios required to be produced for achieving reliable solutions, so that the computational performance might be compromised. Accordingly, the authors in [21] proposed the Wasserstein-metric-based distributionally robust tri-level defense model to mitigate the effects of attacks. However, the performance of this defense model relied heavily on the sample size of wind power output scenarios. The small sample size would lead to the issue of over-fitting while the over-sized samples would cause the computational burden [22]. Meanwhile, these resilience improving strategies in [19-21] ignored the different considerations of conservatism from various defenders to make adjustable defense decisions. This fact indicated that the conservatism of these defense models could not be controlled by the system operator. Furthermore, these methods did not consider the uncertainty of attacks. That is to say, the defender determined line hardening decisions based on the traditional N-K criterion where K as the attack budget was fixed as a static value.

In reality, the attack uncertainty should also be considered, as the attack budget is not revealed to the defender before attacks are launched. This is because a defender is almost impossible to know the full and accurate attack information. Thus, it is hard to determine effective defense strategies without a clear understanding of the post-attack impact, which is formulated as the total number of lines attacked by an intelligent attacker. The traditional line hardening strategy based on a fixed attack budget may not mitigate against uncertainty of attacks. The authors in [23] pointed out that attack budgets of the attacker could not be accurately known by the defender. In this sense, the authors in [23] proposed an improved tri-level defense model for transmission line protection considering the uncertainty of attack budgets. Meanwhile, the authors in [24] developed a robust defense model to determine the line protection plan against uncertain attacks. A hybrid robust tri-level defense model was proposed in [25] to alleviate the effects of uncertain attacks on power systems. However, these tri-level defense models for line hardening strategies in [23-25] only considered a single source of uncertainty from attacks without further consideration of uncertainty from renewable energy. In practice, the decision-making strategies for the allocation of limited defense resources generally involve the multiple uncertainties in power systems. Notably, this paper focuses on both uncertainties from the attacks as well as the wind power output. Thus, uncertain attacks and uncertain wind power output are formulated together in the defense process to improve the resilience of power systems.

In this paper, an adjustable robust tri-level defender-attacker-defender (ART-DAD) model is proposed to improve the resilience of power systems against uncertain attacks. An adjustable robust technique is developed that can characterize the uncertainty of random variables with limited information, which does not rely on the traditional approach of priori probability distribution function with massive historical information of the random variables. The proposed ART-DAD model can also adjust the conservatism level of system operator decisions. This adjustable robust technique can characterize the uncertainties pertaining to random variables in terms of bounded intervals rather than scenarios, which can effectively improve the computational performance. In addition, a dynamic N-K criterion is developed to capture all possible attack budgets, where attack budgets are formulated as a probabilistic distribution of the total number of attacked lines. Meanwhile, the proposed ART-DAD model can be solved by using a constraint-generation based solution algorithm. Finally, the proposed ART-DAD model is validated to provide viable resilience improving strategies for power systems with high wind power penetration against uncertain attacks. The main contributions of this paper are summarized as follows:

(1) To the best of the authors' knowledge, the previous tri-level defense models do not consider both uncertainties of attacks and wind power output. To fill this gap, an adjustable robust tri-level defender-attacker-defender model is proposed to improve the resilience of power systems with high wind power penetration against uncertain attacks.

(2) The proposed ART-DAD model develops a polyhedral uncertainty set for wind power output and a dynamic N-K criterion for uncertain attack budgets. The proposed model can flexibly formulate the probabilities of attack budgets and adjust the risk-aversion level of the system operator decision by properly setting the level of conservatism in the polyhedral uncertainty set.

(3) To obtain the global optimal solution, the overall ART-DAD model is innovatively decoupled into a master and sub-problem, which can be solved iteratively by a constraint-generation based solution algorithm. In addition, case studies are implemented to verify the performance of the proposed model that enables a more flexible and practical decision in the defense process.

The remaining parts of this paper are organized as follows: Section II provides the mathematical formulation of the proposed ART-DAD model. Section III decouples the ART-DAD model into the master and sub-problem with the constraint-generation based solution algorithm. Section IV implements case studies to verify the effectiveness of the proposed ART-DAD model. Finally, conclusion is drawn in section V.

II. The Adjustable Robust Defender-Attacker-Defender Model

A. The polyhedral uncertainty set for wind power output

The stochastic nature of wind power output can impose a serious impact on the power system with high wind power penetration. In practice, a polyhedral uncertainty set is particularly effective in modeling the uncertainty of random variables, which does not require a specific probability distribution of wind power output [26]. Because the probability information of random variables is difficult to be obtained accurately, this polyhedral uncertainty set can be considered as a better approach to characterize the uncertainty of random variables such as the wind power output [27]. This paper further extends the polyhedral uncertainty set for wind power output in which the defender can adjust the conservatism) of the proposed ART-DAD model. The improved polyhedral uncertainty set for wind power output is formulated as follows:

$$\mathbb{R} = \left\{ P_{\mathrm{W},w} \left| \begin{array}{l} P_{\mathrm{W},w} = \overline{P}_{\mathrm{W},w} + \Delta P_{\mathrm{W},w}\left(\nu_w^+ - \nu_w^-\right) + \\ \Delta P_{\mathrm{W},w}(\Lambda - \vec{\Lambda})\left(\upsilon_w^+ - \upsilon_w^-\right) \\ \sum_{w \in \boldsymbol{W}} \left(\nu_w^+ + \nu_w^-\right) = \vec{\Lambda} \\ \nu_w^+ + \nu_w^- + \upsilon_w^+ + \upsilon_w^- \le 1, \sum_{w \in \boldsymbol{W}} \left(\upsilon_w^+ + \upsilon_w^-\right) = 1 \\ \nu_w^+, \nu_w^-, \upsilon_w^+, \upsilon_w^- \in \{0,1\} \\ \Pi = \Lambda / \mathrm{NW}, \forall w \in \boldsymbol{W} \end{array} \right. \right\} \tag{1}$$

where $\Delta P_{\mathrm{W},w}$ is set to the largest variation of the expected wind power output $\overline{P}_{\mathrm{W},w}$. This is to include more extreme scenarios of wind power output. The first and second rows in equation (1) represent the value of the wind power output $P_{\mathrm{W},w}$ based on the forecast and fluctuation levels. The third row in equation (1) defines the number of extreme points in $\mathbb{R}$. The fourth row in equation (1) ensures that $P_{\mathrm{W},w}$ cannot be at both upper and lower bounds at the same time. The fifth row in equation (1) defines the binary variables ν_w^+, ν_w^-, υ_w^+, and υ_w^- that are introduced to limit wind power output $P_{\mathrm{W},w}$ within the ideal interval $[\overline{P}_{\mathrm{W},w} - \Delta P_{\mathrm{W},w}, \overline{P}_{\mathrm{W},w} + \Delta P_{\mathrm{W},w}]$. Π represents the uncertainty budget which can adjust the conservatism of defense model. As Π increases, the size of the polyhedral uncertainty set enlarges. This means that the total deviation from the expected wind power output becomes larger, so that the defense strategy is considered to be more conservative, and the system is protected against a higher degree of uncertainty. Here, Π =0 means that no uncertainty is considered for $P_{\mathrm{W},w}$, while Π =1 indicates that the optimization model only considers the worse-case scenario for $P_{\mathrm{W},w}$. Notably, Λ is introduced as an auxiliary parameter, which can be fractional, and $\vec{\Lambda}$ is the integer and rounded down value of Λ.

B. Dynamic N-K criterion for uncertain attacks

The line disruption is often applied to describe the impact of attacks on power systems. This is formulated as the static N-K criterion as follows:

$$\sum_{l=1}^{N_{\mathrm{L}}}(1-a_l)\le R_{\mathrm{A}} \qquad \forall a_l\in\{0,1\} \tag{2}$$

where a_l is a binary variable, which represents the status of line l. If a_l is equal to 0, line l is disrupted due to attacks, otherwise line l is not attacked. Equation (2) denotes that the attacker can choose up to R_{A} number of lines to launch an attack. R_{A} also denotes as the attack budget. Notably, R_{A} in (2) is generally set to a static value based on historical data.

The system operator is often not able to obtain the accurate information associated with attack budget R_{A}, as its value cannot be accurately known by the defender. This implies that attack budget R_{A} should be a dynamic value rather than a static one. In this paper, the attack budget is innovatively formulated as a dynamic problem, so that a set of attack budgets is adopted to describe the uncertainty of attack budgets as follows:

$$\sum_{l\in\boldsymbol{L}}(1-a_l(s))\le R_{\mathrm{A}}(s) \quad \forall a_l(s)\in\{0,1\}, s\in\boldsymbol{S} \tag{3}$$

where $a_l(s)$ is a binary variable for attack decision of line l in attack budget scenario s. Similarly, if $a_l(s)$ equals 0, line l is under attack in attack budget scenario s, otherwise line l remains un-attacked in the attack budget scenario s. $R_{\mathrm{A}}(s)$ represents the total number of lines to be attacked in the attack budget scenario s, which reflects the uncertainty of attacks. $\boldsymbol{S}$ is a set of attack budget scenarios. This dynamic formulation means that the total number of lines attacked is not a fixed value, but a probabilistic distribution over a set of attack budgets is used to better model the uncertain attacks. There are four reasonable assumptions in the dynamic N-K criterion for uncertain attacks: 1) the defender and the attacker only harden and attack the power system lines, respectively; 2) the hardened lines cannot be disrupted by an attacker; 3) the attacked lines remain out of service; 4) the system operator can reasonably generate a set of attack budget scenarios based on historical data.

C. The Adjustable Robust Tri-level Defense Model

The proposed ART-DAD model can be defined as a tri-level defense framework, as shown in Fig. 1. This optimal defense strategy is achieved by minimizing the total expected costs that are the sum of the line hardening cost and the expected operation cost. In the upper-level, the defender makes an optimal defense decision of line hardening strategy with a limited defense resource, aiming to minimize the cost of hardening lines. In the mid-level, the attacker disrupts the transmission lines in order to maximize the expected operation cost by considering all possible attack budget scenarios and their corresponding probabilities, as well as the wind power output uncertainty. In the lower-level, after each attack, the system operator takes dispatch actions to mitigate the attack impacts. This is achieved by optimizing the power flow through unit dispatch and load shedding to minimize the system operation cost under each attack budget scenario. The systems operation cost includes both generation dispatch and load shedding costs.

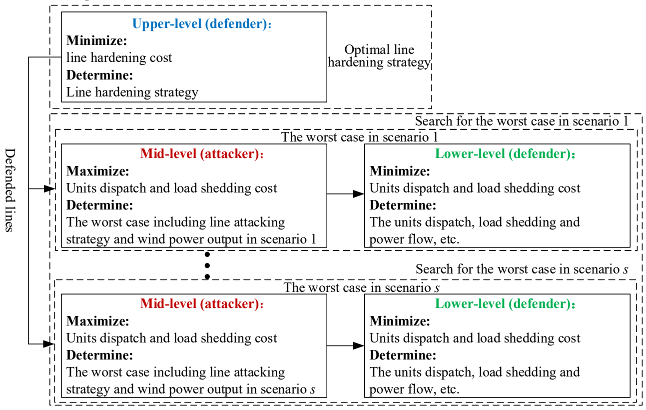


Fig. 1. Framework of the proposed adjustable robust tri-level defense model.

Hence, the mathematical formulation of the proposed ART-DAD model can be described as follows:

Upper-level:

$$\min_{d_l}\sum_{l\in\boldsymbol{L}}C_{\mathrm{L}l}d_l \tag{4}$$

subject to:

$$\sum_{l\in\boldsymbol{L}}d_l\le R_{\mathrm{L}} \qquad \forall d_l\in\{0,1\} \tag{5}$$

where d_l is a binary variable which represents the status of line l. If $d_l=1$, line l is hardened by the defender so that the attacker cannot disrupt this line. Otherwise, $d_l=0$ represents that line l is not protected and it is vulnerable to a potential attack. Notably, equation (4) indicates the upper-level objective function of the proposed ART-DAD model to minimize the cost of hardening lines.

Mid-level:

$$\max_{a_l(s),P_{\mathrm{W}_w}(s)\in\mathbb{R}}\Xi(P_{\mathrm{G}}(s),\Delta P_{\mathrm{D}d}(s)) \tag{6}$$

subject to:

$$\mathbb{R}=\left\{P_{\mathrm{W},w}\left|\begin{array}{l} P_{\mathrm{W},w}=\bar{P}_{\mathrm{W},w}+\Delta P_{\mathrm{W},w}\left(\nu_w^+-\nu_w^-\right)+\\ \Delta P_{\mathrm{W},w}(\Lambda-\vec{\Lambda})\left(\upsilon_w^+-\upsilon_w^-\right)\\ \sum_{w\in\boldsymbol{W}}\left(\nu_w^++\nu_w^-\right)=\vec{\Lambda}\\ \nu_w^++\nu_w^-+\upsilon_w^++\upsilon_w^-\le 1,\ \sum_{w\in\boldsymbol{W}}\left(\upsilon_w^++\upsilon_w^-\right)=1\\ \nu_w^+,\nu_w^-,\upsilon_w^+,\upsilon_w^-\in\{0,1\}\\ \Pi=\Lambda/\mathrm{NW},\forall w\in\boldsymbol{W} \end{array}\right.\right\} \tag{7}$$

$$\sum_{l\in\boldsymbol{L}}(1-a_l(s))\le R_{\mathrm{A}}(s) \qquad \forall a_l(s)\in\{0,1\}, s\in\boldsymbol{S} \tag{8}$$

where equation (6) defines the mid-level objective function for the proposed ART-DAD model. Objective (6) maximizes the expected operation cost. In addition, the uncertainty set (7) is used to formulate wind power output uncertainty with all possible extreme scenarios for wind power output. Lines are assumed as the only assets to be attacked and defended, respectively. Thus, the constraint corresponding to the line disruption is formulated as the attack model. Equation (8) represents the uncertainty set of all possible N-K contingencies, which is formulated as the attack budget scenarios with their corresponding probabilities.

Lower-level:

$$\Xi(P_{Gi},\Delta P_{Dd}) = \min_{\substack{P_{Gi}(s),P_{Fl}(s),\\ \theta_b(s),\Delta P_{Dd}(s)}} \left[\sum_{i\in \boldsymbol{G}} C_{Gi}P_{Gi}(s) + \sum_{d\in \boldsymbol{D}} C_{Dd}\Delta P_{Dd}(s)\right] \quad (9)$$

subject to:

$$\begin{aligned}&\sum_{l\in \boldsymbol{L}} \boldsymbol{K}_{\boldsymbol{L}b,l} P_{Fl}(s) + \sum_{d\in \boldsymbol{D}} \boldsymbol{K}_{\boldsymbol{D}b,d}\left(P_{Dd}^{\max} - \Delta P_{Dd}(s)\right) = \\ &\sum_{i\in \boldsymbol{G}} \boldsymbol{K}_{\boldsymbol{P}b,i} P_{Gi}(s) + \sum_{w\in \boldsymbol{W}} \boldsymbol{K}_{\boldsymbol{W}b,w} P_{Ww}(s) \quad \forall b\in \boldsymbol{B}\end{aligned} \quad (10)$$

$$P_{Fl}(s) = \left[1-(1-d_l)(1-a_l(s))\right] X_l^{-1} \boldsymbol{K}_{\boldsymbol{L}l}^{\mathrm{T}} \boldsymbol{\theta}(s) \quad \forall l\in \boldsymbol{L}, \forall b\in \boldsymbol{B}, \forall s\in \boldsymbol{S} \quad (11)$$

$$0 \le P_{Gi}(s) \le P_{Gi}^{\max} \quad \forall i\in \boldsymbol{G}, \forall s\in \boldsymbol{S} \quad (12)$$

$$0 \le \Delta P_{Dd}(s) \le P_{Dd}^{\max} \quad \forall d\in \boldsymbol{D}, \forall s\in \boldsymbol{S} \quad (13)$$

$$-P_{Fl}^{\max} \le P_{Fl}(s) \le P_{Fl}^{\max} \quad \forall l\in \boldsymbol{L}, \forall s\in \boldsymbol{S} \quad (14)$$

$$-\theta_b^{\max} \le \theta_b(s) \le \theta_b^{\max} \quad \forall b\in \boldsymbol{B}, \forall s\in \boldsymbol{S} \quad (15)$$

where equation (9) indicates the lower-level objective function of the proposed ART-DAD model. Objective (9) minimizes the system operation cost for generation dispatch and load shedding in each attack budget scenario *s,* which follows the dispatch actions from the system operator. Equation (10) ensures the power balance for bus *b* in each attack budget scenario *s*. Equation (11) indicates the power flow for line *l* in each attack budget scenario *s*, which incorporates the impacts of defense and attack decisions. If d_l=1 and $a_l(s)$=1, or d_l=0 and $a_l(s)$ =1, line *l* is not attacked in the attack budget scenario *s*. If d_l=1 and $a_l(s)$=0, line *l* is hardened so that it cannot be disrupted in attack budget scenario *s*. If d_l=0 and $a_l(s)$=0, line *l* is not hardened and attacked in the attack budget scenario *s*. Equation (12) is the generation capacity limit constraint for unit *i* in each attack budget scenario. Equation (13) represents the load shedding capacity limit constraint for load *d* in each attack budget scenario. Equation (14) denotes the power flow capacity limit constraint for line *l* in each attack budget scenario. Equation (15) indicates the bus voltage angle capacity limit constraint for bus *b* in each attack budget scenario *s*.

Finally, the proposed ART-DAD model can be formulated as a mixed-integer tri-level programming problem with the objective (16), which is subject to the constraint (5) in the upper-level, the constraints (7), (8) in the mid-level, and (10)-(15) in the lower-level. Then, the mixed-integer tri-level programming problem can be solved by the constraint-generation based solution algorithm with a master and sub-problem scheme, which will be discussed in the following section.

$$\begin{aligned}&\min_{d_l} \sum_{l\in \boldsymbol{L}} C_{Ll} d_l + \\ &E_{\Omega(s)}\left[\max_{a_l(s),P_{Ww}(s)} \min_{\substack{P_{Gi}(s),P_{Fl}(s),\\ \theta_b(s),\Delta P_{Dd}(s)}} \left(\sum_{i\in \boldsymbol{G}} C_{Gi}P_{Gi}(s) + \sum_{d\in \boldsymbol{D}} C_{Dd}\Delta P_{Dd}(s)\right)\right]\end{aligned} \quad (16)$$

III. Solution Methodology

In this section, the proposed ART-DAD model is decoupled into a master and sub-problem, which is then iteratively solved by the constraint-generation based solution algorithm to obtain an optimal defense strategy. The detailed formulation of the master and sub-problem is given in the following subsection.

A. Master Problem Formulation

Given $\widehat{\boldsymbol{A}}$, the defender minimizes the total expected costs for a power system. Note here, $\widehat{\boldsymbol{A}}$ contains a set of the worst-case attack budget scenario and extreme wind power output scenarios, which are presented as follows:

$$\widehat{\boldsymbol{A}} = [\widehat{\boldsymbol{A}}_1, \ldots, \widehat{\boldsymbol{A}}_k, \ldots, \widehat{\boldsymbol{A}}_m] \quad k=1, 2, \ldots, m \quad (17)$$

where *m* represents the number of iterations in the solution process; the sign "^" denotes that the value of a variable is given. In (17), $\widehat{\boldsymbol{A}}_k$ is equal to $[\widehat{\boldsymbol{A}}_k(1), \ldots, \widehat{\boldsymbol{A}}_k(ns), \ldots, \widehat{\boldsymbol{A}}_k(Ns)]$, in which Ns is the total number of all possible attack budget scenarios, and *ns* represents the *ns*th attack budget scenario. For a given $\widehat{\boldsymbol{A}}_k(ns)$ in attack budget scenario *s*, we have $\widehat{\boldsymbol{A}}_k(ns) = [\hat{a}_{l,k}(s), \hat{P}_{Ww,k}(s)]|_{l\in \boldsymbol{L}, w\in \boldsymbol{W}}$. Based on $\widehat{\boldsymbol{A}}$, the master problem can be formulated as follows:

$$\rho = \min_{d_l} \sum_{l\in \boldsymbol{L}} C_{Ll} d_l + \omega \quad (18)$$

subject to:

$$\sum_{l\in \boldsymbol{L}} d_l \le R_L \quad \forall d_l \in \{0,1\} \quad (19)$$

$$\omega \ge \sum_{s\in \boldsymbol{S}}\left[\Omega(s)\left(\sum_{i\in \boldsymbol{G}} C_{Gi}P_{Gi,k}(s) + \sum_{d\in \boldsymbol{D}} C_{Dd}\Delta P_{Dd,k}(s)\right)\right] \quad \forall k = 1,2,\ldots,m \quad (20)$$

$$-\left(1-\hat{a}_{l,k}(s)\right)(1-d_l)M \le P_{Fl,k}(s) - X_l^{-1}\boldsymbol{K}_{Ll}^{\mathrm{T}}\boldsymbol{\theta}_k(s) \quad \forall l\in \boldsymbol{L}, \forall b\in \boldsymbol{B}, \forall s\in \boldsymbol{S}, \forall k = 1,2,\ldots,m \quad (21)$$

$$P_{Fl,k}(s) - X_l^{-1}\boldsymbol{K}_{\boldsymbol{L}}^{\mathrm{T}}\boldsymbol{\theta}_k(s) \le \left(1-\hat{a}_{l,k}(s)\right)(1-d_l)M \quad \forall l\in \boldsymbol{L}, \forall b\in \boldsymbol{B}, \forall s\in \boldsymbol{S}, \forall k = 1,2,\ldots,m \quad (22)$$

$$\begin{aligned}&\sum_{l\in \boldsymbol{L}} \boldsymbol{K}_{\boldsymbol{L}b,l} P_{Fl,k}(s) + \sum_{d\in \boldsymbol{D}} \boldsymbol{K}_{\boldsymbol{D}b,d}\left(P_{Dd}^{\max} - \Delta P_{Dd,k}(s)\right) = \\ &\sum_{i\in \boldsymbol{G}} \boldsymbol{K}_{\boldsymbol{P}b,i} P_{Gi,k}(s) + \sum_{w\in \boldsymbol{W}} \boldsymbol{K}_{\boldsymbol{W}b,w} \hat{P}_{Ww,k}(s) \quad \forall b\in \boldsymbol{B}\end{aligned} \quad (23)$$

$$0 \le P_{Gi,k}(s) \le P_{Gi}^{\max} \quad \forall i\in \boldsymbol{G}, \forall s\in \boldsymbol{S}, \forall k = 1,2,\ldots,m \quad (24)$$

$$0 \le \Delta P_{Dd,k}(s) \le P_{Dd}^{\max} \quad \forall d\in \boldsymbol{D}, \forall s\in \boldsymbol{S}, \forall k = 1,2,\ldots,m \quad (25)$$

$$-\theta_b^{\max} \le \theta_{b,k}(s) \le \theta_b^{\max} \quad \forall b\in \boldsymbol{B}, \forall s\in \boldsymbol{S}, \forall k = 1,2,\ldots,m \quad (26)$$

$$-\left(\hat{a}_{l,k}(s)P_{Fl}^{\max} + \left(1-\hat{a}_{l,k}(s)\right)d_l P_{Fl}^{\max}\right) \le P_{Fl,k}(s) \quad \forall l\in \boldsymbol{L}, \forall s\in \boldsymbol{S}, \forall k = 1,2,\ldots,m \quad (27)$$

$$P_{Fl,k}(s) \le \hat{a}_{l,k}(s)P_{Fl}^{\max} + \left(1-\hat{a}_{l,k}(s)\right)d_l P_{Fl}^{\max} \quad \forall l\in \boldsymbol{L}, \forall s\in \boldsymbol{S}, \forall k = 1,2,\ldots,m \quad (28)$$

where *M* represents a large positive constant; ω is an auxiliary continuous variable. *m* represents the number of iterations in the proposed solution algorithm. For each iteration *k*, new constraints (20)-(28) are added into the master problem with variables $P_{Gi,k}(s)$, $\Delta P_{Dd,k}(s)$, $P_{Fl,k}(s)$, $\theta_{b,k}(s)$ in attack budget scenario s respectively. This is to provide an updated line hardening strategy for each iteration.

B. Sub-problem Formulation

The sub-problem calculates the expected operation cost for the system by considering all possible attack budgets, which can be described as follows:

$$\omega=\sum_{s\in\boldsymbol{S}}\left(\Omega(s)\Theta(s)\right) \tag{29}$$

where ω is the expected operation cost for the system in all possible attack budgets. $\Theta(s)$ denotes the system operation cost in attack budget scenario s, which is composed of unit dispatch and load shedding costs. $\Omega(s)$ defines the probability of attack budget scenario s.

It should point out that in each attack budget scenario, the attacker's objective is to maximize the attack impacts by mean of system operation cost, while the defender aims to minimize the system operation cost caused by the attack. Thus, the trade-off between the attacker and the system operator in each attack budget scenario can be formulated as a bi-level game problem as follows:

$$\max_{a_l(s),P_{\mathrm{W}w}(s)\in\mathbb{R}} \Theta(s) \tag{30}$$

subject to: (7) and (8)

$$\Theta(s)=\min_{\substack{P_{\mathrm{G}i}(s),\Delta P_{\mathrm{D}d}(s),\\ P_{\mathrm{F}l}(s),\theta_b(s)}}\left(\sum_{i\in\boldsymbol{G}}C_{\mathrm{G}i}P_{\mathrm{G}i}(s)+\sum_{d\in\boldsymbol{D}}C_{\mathrm{D}d}\Delta P_{\mathrm{D}d}(s)\right) \tag{31}$$

Subject to:

$$\begin{aligned}&\sum_{l\in\boldsymbol{L}}\boldsymbol{K}_{\boldsymbol{L}b,l}P_{\mathrm{F}l}(s)+\sum_{d\in\boldsymbol{D}}\boldsymbol{K}_{\boldsymbol{D}b,d}\left(P_{\mathrm{D}d}^{\max}-\Delta P_{\mathrm{D}d}(s)\right)=\\&\sum_{i\in\boldsymbol{G}}\boldsymbol{K}_{\boldsymbol{P}b,i}P_{\mathrm{G}i}(s)+\sum_{w\in\boldsymbol{W}}\boldsymbol{K}_{\boldsymbol{W}b,w}P_{\mathrm{W}w}(s)\quad(\lambda_b(s))\ \forall b\in\boldsymbol{B}\end{aligned} \tag{32}$$

$$P_{\mathrm{F}l}(s)=[1-(1-\hat{d}_l)(1-a_l)]X_l^{-1}\boldsymbol{K}_{\boldsymbol{L}l}^{\mathrm{T}}\boldsymbol{\theta}(s)\quad(\mu_l(s))\quad \forall l\in\boldsymbol{L},\forall b\in\boldsymbol{B},\forall s\in\boldsymbol{S} \tag{33}$$

$$0\le P_{\mathrm{G}i}(s)\le P_{\mathrm{G}i}^{\max}\qquad(\overline{\gamma}_i(s))\ \forall i\in\boldsymbol{G},\forall s\in\boldsymbol{S} \tag{34}$$

$$0\le \Delta P_{\mathrm{D}d}(s)\le P_{\mathrm{D}d}^{\max}\qquad(\overline{\alpha}_d(s))\quad \forall d\in\boldsymbol{D},\forall s\in\boldsymbol{S} \tag{35}$$

$$-P_{\mathrm{F}l}^{\max}\le P_{\mathrm{F},l}(s)\le P_{\mathrm{F}l}^{\max}\ \left(\underline{\varphi}_l(s),\overline{\varphi}_l(s)\right)\ \forall l\in\boldsymbol{L},\forall s\in\boldsymbol{S} \tag{36}$$

where $\lambda_b(s)$, $\mu_l(s)$, $\overline{\gamma}_i(s)$ and $\overline{\alpha}_d(s)$ represent dual variables associated with constraints (32)-(35), respectively; $\underline{\varphi}_l(s)$ and $\overline{\varphi}_l(s)$ are dual variables associated with lower and upper constraint (36). Since the sub-problem is a max-min problem, the duality theory is applied to convert this max-min sub-problem into a single problem. For simplicity but without loss of generality, the sign (s) that denotes the attack budget scenario s is omitted. The converted sub-problem is formulated as follows:

$$\begin{aligned}\tau=\max&\sum_{l\in\boldsymbol{L}}(\overline{\varphi}_l-\underline{\varphi}_l)P_{\mathrm{F}l}^{\max}-\sum_{w\in\boldsymbol{W}}\boldsymbol{\lambda}^{\mathrm{T}}\boldsymbol{K}_{\boldsymbol{W},w}P_{\mathrm{W}w}+\\&\sum_{i\in\boldsymbol{G}}\overline{\gamma}_iP_{\mathrm{G}i}^{\max}+\sum_{d\in\boldsymbol{D}}(\overline{\alpha}_d+\boldsymbol{\lambda}^{\mathrm{T}}\boldsymbol{K}_{\boldsymbol{D},d})P_{\mathrm{D}d}^{\max}\end{aligned} \tag{37}$$

subject to:

(7) and (8) (38)

$$\sum_{l\in\boldsymbol{L}}[(1-\hat{d}_l)X_l^{-1}\boldsymbol{K}_{\boldsymbol{L}l,b}^{\mathrm{T}}\cdot a_l\mu_l+\hat{d}_lX_l^{-1}\boldsymbol{K}_{\boldsymbol{L}l,b}^{\mathrm{T}}\mu_l]=0\quad\forall b\in\boldsymbol{B} \tag{39}$$

$$-\sum_{b\in\boldsymbol{B}}\boldsymbol{K}_{\boldsymbol{L}l,b}^{\mathrm{T}}\lambda_b+\mu_l+\overline{\varphi}_l+\underline{\varphi}_l=0\qquad\forall l\in\boldsymbol{L} \tag{40}$$

$$\sum_{b\in\boldsymbol{B}}\boldsymbol{K}_{\boldsymbol{P}i,b}^{\mathrm{T}}\lambda_b+\overline{\gamma}_i\le C_{\mathrm{G}i}\qquad\forall i\in\boldsymbol{G} \tag{41}$$

$$\sum_{b\in\boldsymbol{B}}\boldsymbol{K}_{\boldsymbol{D}d,b}^{\mathrm{T}}\lambda_b+\overline{\alpha}_d\le C_{\mathrm{D}d}\qquad\forall d\in\boldsymbol{D} \tag{42}$$

$$\overline{\gamma}_i\le0,\overline{\alpha}_d\le0,\overline{\varphi}_l\le0,\underline{\varphi}_l\ge0\quad\forall i\in\boldsymbol{G},\forall d\in\boldsymbol{D},\forall l\in\boldsymbol{L} \tag{43}$$

$$\lambda_b\text{: free},\ \mu_l\text{: free}\qquad\forall b\in\boldsymbol{B},\forall l\in\boldsymbol{L} \tag{44}$$

Based on the dual theory, equation (37) is equal to the original equation (31). Constraint (38) indicates that the total number of attacked lines is no more than the attack budget. Dual constraints (39)-(42) are corresponding to the decision variables θ_b , $P_{\mathrm{F},l}$, $P_{\mathrm{G},i}$ and $\Delta P_{\mathrm{D}d}$ in attack budget scenario s, respectively. Constraints (43)-(44) confine the dual variables.

There are nonlinear terms in equations (37) and (39). Specifically, the nonlinear term in (37) is $\boldsymbol{\lambda}^{\mathrm{T}}\boldsymbol{K}_{\boldsymbol{W},w}P_{\mathrm{W}w}$, and the nonlinear term in (39) is a bilinear term $a_l\mu_l$. Based on (7), $\boldsymbol{\lambda}^{\mathrm{T}}\boldsymbol{K}_{\boldsymbol{W},w}P_{\mathrm{W}w}$ can be transformed into a bilinear term $\eta_w[\overline{P}_{\mathrm{W},w}+\Delta P_{\mathrm{W},w}(\nu_w^+-\nu_w^-)+\Delta P_{\mathrm{W},w}(\Lambda-\bar{\Lambda})(\upsilon_w^+-\upsilon_w^-)]$, where η_w is equal to $\boldsymbol{\lambda}^{\mathrm{T}}\boldsymbol{K}_{\boldsymbol{W},w}$. Note that the bilinear term is defined as the multiplication of a binary variable and a continuous variable, which can be linearized by the big-M method. Following this method, the big-M method is adopted to linearize $a_l\mu_l$ as follows:

$$\begin{cases}t_l=a_l\mu_l & \forall l\in\boldsymbol{L}\\ t_l\ge -Ma_l & \forall l\in\boldsymbol{L}\\ t_l\le Ma_l & \forall l\in\boldsymbol{L}\\ t_l\ge\mu_l+Ma_l-M & \forall l\in\boldsymbol{L}\\ t_l\le\mu_l-Ma_l+M & \forall l\in\boldsymbol{L}\end{cases} \tag{45}$$

Finally, the sub-problem is converted into a mixed-integer linear programming (MILP) model, which can be directly solved by a suitable solver. Notably, the appendix A gives the overall framework of the constraint-generation based solution algorithm for solving the proposed ART-DAD model.

IV. Case Study

In this section, extensive numerical simulations are carried out on the proposed ART-DAD model and the constraint-generation based solution algorithm for two modified IEEE RTS-79 and RTS-96 systems [28]. The proposed ART-DAD model in various case studies is solved using CPLEX 12.4 solver on a workstation with an i9-13900KS Processor (3.2GHz) and 96 GB RAM. Notably, the attack budget scenarios and probabilities can be rationally assumed by defender based on historical data, which can be achieved and demonstrated in [23, 24].

IEEE RTS-79 System: This IEEE RTS-79 system consists of 24 buses, 17 loads, 38 transmission lines, and 10 generators with a total generation capacity of 3,405 MW. The total system load is set at 2,850 MW. In this system, there are 6 wind farms connected to buses 1, 5, 9, 13, 17 and 21 respectively with a

50% penetration level, which is defined as the installed wind capacity divided by total load. In addition, the line hardening cost for each line is set at 400$/meter, and the load loss cost is 150$/MW.

A. Effectiveness Tests of the Proposed ART-DAD Model

Case 1: This case analyzes the effectiveness of the proposed ART-DAD model comparing with the hybrid robust and robust defense models on the RTS-79 system. As a typical attack case, an intelligent cyber-attacker is able to intrude the power system and exploit the vulnerabilities in the supervisory control and data acquisition system to disrupt the transmission lines. In practice, the cyber-attacker may attack on communication links to induce power outages and increase the system operation cost. However, it is infeasible for a defender to accurately know the attack budgets that is launched by an intelligent attacker. Thus, an uncertain attack is introduced with a set of attack budget scenarios and probability. In this case study, it is assumed that historical information on cyber-attacks could enable the system operator to estimate that an attacker has a 0.6 probability of disrupting three lines and a 0.4 probability of disrupting five lines. That is, the possible attack budget set is estimated as $\boldsymbol{S}$= (3, 5) with probabilities Ω= (0.6, 0.4). In addition, the defense resource is assumed to be four defended lines, i.e., R_L=4, and the uncertainty budget Π is set at 0.6. Tables I-II show the simulation results.

Table I shows the simulation results of the ART-DAD model to defend the defined uncertain attacks $\boldsymbol{S}$= (3, 5) with probabilities Ω= (0.6, 0.4). It can be seen that the four hardened lines are 1, 9, 25, and 28 based on the proposed ART-DAD model. The total expected costs are 91,272.99$, calculated as the sum of the line hardening cost and the expected operation cost. Notably, the expected operation cost is equal to the weighted sum of each operation cost and the corresponding probability. It can be found that the system operation cost in certain single attack budget may not achieve the most optimal solution, but the expected operation costs for all possible attack budgets reach the minimal value as the global optimal solution of defense strategy. This is because the proposed ART-DAD model aims to minimize the total expected costs in all possible attack budget scenarios.

TABLE I
LINE HARDENING STRATEGY AND COSTS FOR UNCERTAIN ATTACKS WITH PROBABILITY DISTRIBUTION

This paper	R_A=3	R_A=5
Attacked lines	29,36,37	18,20,21,23,27
Operation cost ($)	69,318.72	120,204.39
Total expected costs	91,272.99$=4×400+69,318.72×0.6+120,204.39×0.4	
Defended lines	1,9,25,28	

Table II presents the comparative simulation results to verify the advantage of the proposed ART-DAD model, which is over the hybrid robust defense model and the robust defense model. In the hybrid robust model, protected lines 1, 3, 25, 28 are optimally selected by considering all possible attack budgets with the worst-case wind power output scenario. The total expected costs are calculated as 91,617.61$, which is more expensive than 91,272.99$ obtained by the proposed ART-DAD model. If the robust defense model is applied to determine the optimal defense strategy, the total expected costs will reach up to 95,418.92$. This is because the robust defense model only considers the worst-case scenario, resulting in a high-cost decision. The comparison of simulation results means that the proposed ART-DAD model is more effective than other traditional defense models in terms of total expected costs. This fact indicates that the line hardening strategy developed by the proposed ART-DAD model can effectively mitigate the impacts of uncertain attacks in power systems by considering the probability distribution of the uncertain attack scenarios.

TABLE II
COMPARATIVE RESULTS FOR DIFFERENT DEFENSE MODELS WITH LINE HARDENING STRATEGIES AND COSTS

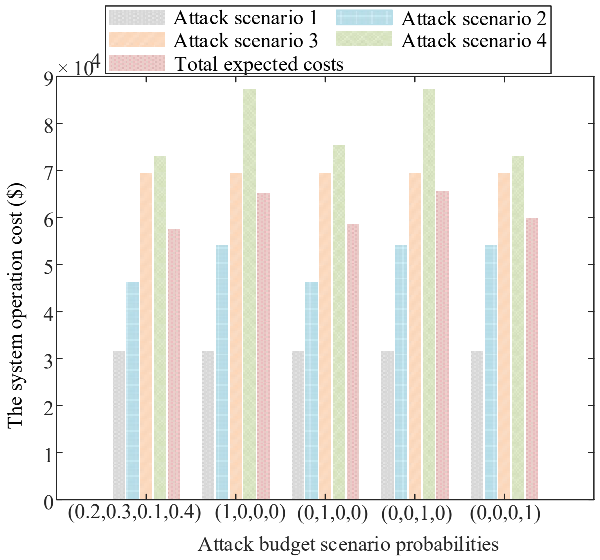
Models	Defended lines	Operation cost ($)		Total expected costs ($)
		R_A=3	R_A=5	
This paper	1,9,25,28	69,318.72	120,204.39	91,272.99
		91,272.99=4×400+69,318.72×0.6+120,204.39×0.4		
Hybrid robust	1,3,25,28	69,685.63	120,515.59	91,617.61
		91,617.61=4×400+69,685.63×0.6+120,515.59×0.4		
Robust model	9,23,31,38	0	93,818.92	95,418.92
		95,418.92=4×400+93,818.92×1		

Case 2: This case further verifies the proposed ART-DAD model can adjust the line hardening strategies against different attack budget scenarios, so that the proposed model is adaptive to various uncertain attacks. Besides cyber-attacks which are able to disrupt transmission lines, physical attacks (e.g., natural disasters or human-made physical attacks) can also directly disrupt power system lines, which will lead to significant financial losses. The system operator may not accurately know the total number of lines that an intelligent attacker can disrupt. Here, the attack budget scenarios are evaluated as a set $\boldsymbol{S}$= (1, 2, 3, 4) with the corresponding probabilities (0.2, 0.3, 0.1, 0.4). The uncertainty budget Π is set at 0.7. In addition, the defense resource R_L is set at 3.

TABLE III
LINE HARDENING STRATEGIES FOR UNCERTAIN ATTACKS WITH DIFFERENT ATTACK BUDGET SCENARIOS.

Type	Defended lines	Attacked lines			
		R_A=1	R_A=2	R_A=3	R_A=4
This paper	9,23,28	11	5,10	29,36,37	11,29,36,37
Scenario 1	9,28	11	19,23	29,36,37	21,22,23,27
Scenario 2	9,23,30	11	5,10	29,36,37	11,25,26,28
Scenario 3	1,2,28	11	19,23	29,36,37	21,22,23,27
Scenario 4	9,21,28	11	19,23	29,36,37	19,23,27,29

As shown in Table III, the line hardening strategy is {9, 23, 28} determined by the proposed ART-DAD model, in which the defender considering all possible attack budget scenarios $\boldsymbol{S}$= (1, 2, 3, 4) with the corresponding probabilities (0.2, 0.3, 0.1, 0.4). As a comparison, Table III shows the detailed simulation results of different defended lines for each specific attack budget scenario. In summary, it can be found that the defender can determine different defended lines based on different attack budgets. The optimal line hardening strategy is {9, 23, 30} based on the single attack budget scenario 2 (i.e., only considering attack budget with two lines) while the defended lines become {9, 28} based on single attack budget scenario 3 (i.e., only considering attack budget with three lines). If the defender only considers the worst-case attack budget (i.e., only attacking four lines), the determined line hardening strategy changes to {9, 21, 28}. Moreover, an interesting observation from Table III is that the total amount of defended lines is two based on the single attack budget scenario 1 (i.e., only considering attack budget with one line), which indicates that the number of defended lines can be reduced with less attack budget. Comparative simulation results verify the adaptivity of line hardening strategy under different attack budget scenarios. In addition, Fig. 2 shows the total expected costs associated with different attack budget scenarios. It can be observed that the total expected costs based on all possible attack budget scenarios (i.e., the corresponding probabilities are (0.2, 0.3, 0.1, 0.4)) reach the minimal values comparing to other single attack budget scenarios. The proposed ART-DAD model can minimize the total expected costs if multiple attack budget scenarios with probabilities are considered. This means that the proposed approach has a better performance against uncertain attacks.



† (Scenario 1: (1,0,0,0); Scenario 2: (0,1,0,0); Scenario 3: (0,0,1,0); Scenario 4: (0,0,0,1))

Fig. 2. System operation costs for different attack budget scenarios.

B. Impact of the Uncertainty Budget

Case 3: This case investigates the impact of the uncertainty budget Π on the line hardening strategy of the proposed ART-DAD model. In practice, the uncertainty budget Π defines the level of conservatism in wind uncertainty, which can regulate the total number of extreme scenarios for wind power output. The uncertainty budget Π varies from 0 to 0.9 with step 0.1. If Π is 0, the value of wind power output is equal to the predicted value with no uncertainty. When the Π increases, more extreme scenarios for wind power output are introduced to reflect the larger uncertainty with less conservatism level. In addition, a set of attack budgets is assumed as $\boldsymbol{S}$= (3, 5) with probabilities (0.7, 0.3). The defense resource R_L is set at 4 (i.e., defended four lines).

Table IV shows the total expected costs and defended lines for line hardening strategy under different uncertainty budgets of wind power output. In each uncertainty budget Π, the system operation cost is calculated under two different attack budget scenarios (i.e., R_A=3 and R_A=5). It can be found that the total expected costs raise as the uncertainty budget Π increases. By increasing the uncertainty budget Π, more extreme scenarios are contained in the uncertainty set of wind power output, resulting in higher total expected costs. However, the total expected costs are always less than the defense model considering the worst-case wind power output scenario in [29]. The proposed ART-DAD model is also compatible with the worst-case wind power output scenario by setting the uncertainty budget Π to 1. These results effectively verify the benefits of the proposed ART-DAD model in reducing the total expected costs, as the proposed model considers the uncertainty set for wind power output rather than the worst-case scenario. These results also show the increase trend in the total expected costs following by the larger uncertainty set of wind power output which contains more extreme scenarios.

In addition, the uncertainty budget Π may affect the line hardening strategy developed by the proposed ART-DAD model. For instance, the defended lines are {1, 3, 25, 30} with the total expected costs 85466.46$ when the uncertainty budget Π is set at 0.4, while the defended lines are {1, 3, 26, 28} with the total expected costs 86,023.82$ if the uncertainty budget Π is 0.5. These results show that the proposed ART-DAD model is able to determine a dynamic line hardening strategy based on different setting of uncertainty budget Π. In addition, it can be observed that the top four defended lines are 1, 3, 26 and 28 in all uncertainty budgets. Thus, the system operator is advised to have priority for hardening lines {1, 3, 26, 28}. In practice, the proposed ART-DAD model can advise the system operator to determine more flexible defense strategies by considering different uncertainty budgets of the wind power output.

TABLE IV
LINE HARDENING STRATEGIES AND COSTS UNDER DIFFERENT UNCERTAINTY BUDGETS OF WIND POWER OUTPUT

Π	Defended lines	Operation cost ($)		Total expected costs ($)
		R_A=3	R_A=5	
0	9,25,28,29	56,188.72	111,157.68	74,279.41
0.1	9,25,28,29	56,409.48	113,216.88	75,051.70
0.2	1,3,28,32	68,576.16	115,208.88	84,165.98
0.3	1,3,31,38	68,775.31	117,066.48	84,862.66
0.4	1,3,25,30	68,965.19	118,636.08	85,466.46
0.5	1,3,26,28	69,150.45	120,061.68	86,023.82
0.6	1,3,26,28	69,318.72	120,204.39	86,184.42
0.7	1,3,26,28	69,481.85	120,342.75	86,340.12
0.8	1,9,25,28	69,634.68	120,472.38	86,485.99
0.9	2,3,26,28	69,773.11	120,582.98	86,616.07
Ref.[29]	2,3,30,32	69,904.33	120,684.07	86,738.25

C. Impact of the Defense Resource

Case 4: This case analyzes the impact of the defense resource R_L (i.e., number of defended lines) on the line hardening strategy of the proposed ART-DAD model. As an example, we assume attack budgets $\boldsymbol{S}$= (3, 4, 5) with probabilities (0.3, 0.2, 0.5). The defense resource R_L varies between 4 and 8 lines with an incremental step of 1 line. The uncertainty budget Π is set at 0.4. Table V shows the impact of different defense resources with the line hardening strategy under various attacks. Fig. 3 shows the total expected costs and individual system operation cost under each defense resource with various attack budget scenarios.

TABLE V
DIFFERENT DEFENSE RESOURCES WITH LINE HARDENING STRATEGY UNDER UNCERTAIN ATTACKS

R_L	Defended lines	Attacked lines		
		R_A=3	R_A=4	R_A=5
4	1,9,25,28	29,36,37	7,21,22,23	7,15,17,18,23
5	1,9,23,25,28	29,36,37	11,29,36,37	7,14,16,20,21
6	1,9,23,28,29,33	11,12,13	25,26,30,31	7,15,17,18,19
7	2,9,11,23,26,28,29	5,10,13	7,19,21,22	18,19,20,21,27
8	2,3,17,21,23,25,28,29	11,12,13	4,5,8,10	5,10,11,12,13

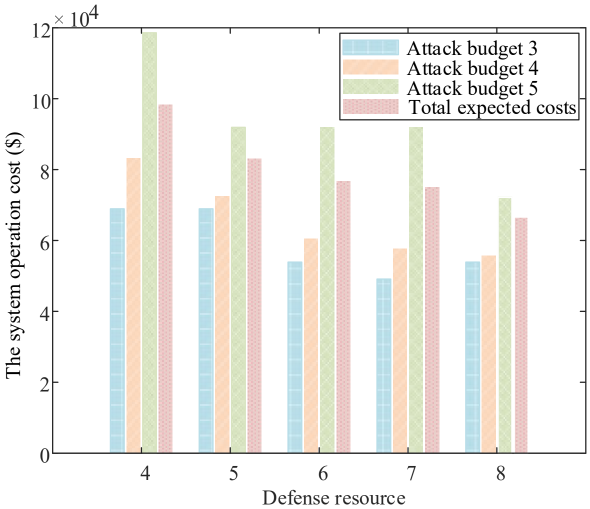


Fig. 3. Impact of defense resource on the total expected and system operation costs.

Table V and Fig. 3 show that the various available defense resources R_L can cause different line hardening strategies with the total expected and system operation costs. In particular, the total expected costs decrease as the defense resource increases. This is because additional critical attacked lines will be defended with the defense resource increase. There are also correlations between different defense resources on the line hardening strategies. For example, as given in Table V, line 23 is attacked when the defense resource R_L is 4. Therefore, line 23 is defended in the new line hardening strategy if the defense resource R_L increases to 5, which allows one additional line 23 to be included in this new line hardening strategy {1, 9, 23, 25, 28}. However, as the defense resource increases, the reduction on the system operation costs will become less effective. For example, when the system operator increases the defense resource from 4 to 8 lines, the system operation costs show a slower reduction trend for all attack budget scenarios. In addition, an interesting observation is that the system operation cost under a specific attack budget may not be effectively reduced when the system operator raises the defense resource. This result is observed in attack budget scenario 3, when the defense resource raises from 7 to 8 lines, the system operation cost will show an opposite and increasing trend. This is due to the optimization objective of the proposed ART-DAD model is to minimize the total expected costs by considering all possible attack budget scenarios.

D. *Impact of the Attack Budget Probabilities*

Case 5: This case conducts the sensitivity analysis of probability distribution amount attack budget scenarios, analyzing the uncertainty related to attack budget probabilities and their impacts on the line hardening strategy of the proposed ART-DAD model. In this case, two possible attack budgets are assumed with four or five lines, R_A=4 or 5 as a set of $\boldsymbol{S}$= (4, 5). Here, the combination of attack budget probabilities is set between (0.1, 0.9) and (0.9, 0.1) with a step change of 0.1. The uncertainty budget Π varies between 0 and 0.8. The system operator has a fixed defense resource to harden four lines, R_L=4.

As shown in Table VI, different distribution of attack budget probabilities can cause various total expected costs for a range of uncertainty budget. Take Π =0.2 as an example, the total expected costs start from the maximum 88,470.74$ when the attack budget probability is (0.1, 0.9), continuously decrease and reach minimum 75,339.00$ for the attack budget probability (0.9, 0.1). The total expected costs are observed to continuously decrease as the probability of 4 attacked lines (R_A=4) outweighs the probability of 5 attacked lines (R_A=5). For all combinations of attack budget probabilities, the total expected costs from the proposed ART-DAD model are still less than that obtained in [29].

TABLE VI
TOTAL EXPECTED COSTS ASSOCIATED WITH VARIOUS DEFENSE STRATEGIES UNDER DIFFERENT ATTACK BUDGET PROBABILITIES

Probabilities	Π =0	Π =0.2	Π =0.4	Π =0.6	Π =0.8	Ref. [29]
(0.1,0.9)	86,688.39	88,470.74	91,586.74	93,033.58	93,306.36	93,350.34
(0.2,0.8)	85,207.78	86,829.28	89,634.08	90,959.43	91,237.01	91,281.77
(0.3,0.7)	83,727.18	85,187.81	87,681.41	88,885.29	89,167.66	89,396.74
(0.4,0.6)	82,246.58	83,546.34	85,728.74	86,811.14	87,098.32	87,144.62
(0.5,0.5)	80,765.97	81,904.87	83,776.08	84,736.99	85,028.97	85,076.05
(0.6,0.4)	79,285.37	80,263.41	81,823.41	82,662.85	82,959.62	83,007.47
(0.7,0.3)	77,804.76	78,621.94	79,870.74	80,588.71	80,890.27	81,142.53
(0.8,0.2)	76,324.16	76,980.47	77,918.08	78,514.56	78,820.93	78,870.32
(0.9,0.1)	74,843.56	75,339.00	75,965.41	76,440.41	76,751.58	76,801.75

Table VII presents the detailed impact of attack budget probabilities on the attacked lines and associated line hardening strategy. These simulation results take the fixed Π =0.4 as an example. Results show that the attack budget probabilities can impact both line hardening strategy and selection of attacked lines. A variation of the attack budget probability could cause the system operator to determine different line hardening strategies. For example, hardened lines are determined as {9, 23, 28, 32} when the attack budget probabilities are (0.3, 0.7), while the hardened lines are {9, 23, 26, 28} if the combination of attack budget probabilities is changed to (0.4, 0.6). However, the defended lines do not change when the attack budget probabilities are ranged between (0.6, 0.4) and (0.9, 0.1). This is due to the attacked lines which mostly remain the same so that the line hardening strategy does not change. The overall results show that the line hardening strategy is less sensitive to the variation of attack budget probabilities. In practice, the proposed ART-DAD model derives an optimal defense strategy that has certain robustness against potential uncertain attacks with various attack budget probabilities.

TABLE VII

SIMULATION RESULTS UNDER DIFFERENT ATTACK BUDGET PROBABILITIES

Type	Defended Lines R_L=4	Attacked Lines R_A=4	Attacked Lines R_A=5	Total expected costs ($)
(0.1,0.9)	9,23,25,28	11,29,36,37	7,14,15,16,17	91,586.74
(0.2,0.8)	9,23,28,33	11,29,36,37	7,14,16,20,21	89,634.08
(0.3,0.7)	9,23,28,32	11,29,36,37	7,14,16,20,21	87,681.41
(0.4,0.6)	9,23,26,28	11,29,36,37	7,15,17,18,19	85,728.74
(0.5,0.5)	9,23,26,28	11,29,36,37	7,15,17,18,19	83,776.08
(0.6,0.4)	9,23,25,28	11,29,36,37	7,14,15,16,17	81,823.41
(0.7,0.3)	9,23,25,28	11,29,36,37	7,14,15,16,17	79,870.74
(0.8,0.2)	9,23,25,28	11,29,36,37	7,14,15,16,17	77,918.08
(0.9,0.1)	9,23,25,28	11,29,36,37	7,14,15,16,17	75,965.41

E. Validation on Large-Scale Power System

IEEE RTS-96 System: To further verify the effectiveness of the proposed ART-DAD model, case studies are implemented on the IEEE RTS-96 system with a total load of 8,550 MW. This is a larger system containing 51 loads, 36 generators, and 120 transmission lines. Similarly, there are 6 wind farms located at buses 1, 15, 29, 43, 57, and 71, respectively. The total installed capacity of wind farms accounts for more than 40% of the total load.

Case 6: In this case study, the attack budget scenarios are assumed to be a set ***S***= (2, 4) with the corresponding probabilities (0.7, 0.3). The defense resource is to harden four lines, i.e., R_L=4. The uncertainty budget is set at Π =0.4. Table VIII-IX present the simulation results of defense strategies and costs with different defense models.

TABLE VIII

SIMULATION RESULTS FOR UNCERTAIN ATTACKS ON THE IEEE RTS-96 SYSTEM

This paper	R_A=2	R_A=4
Attacked lines	5,10	88,100,102,103
Operation cost ($)	133,663.08	153,892.25
Total expected costs	141,331.83$=4×400+133,663.08×0.7+153,892.25×0.3	
Defended lines	25,51,65,104	

TABLE IX

COMPARATIVE RESULTS FOR DIFFERENT DEFENSE MODELS ON THE IEEE RTS-96 SYSTEM

Models	Defended lines	Operation cost ($) R_A=2	Operation cost ($) R_A=4	Total expected costs ($)
This paper	25,51,65,104	133,663.08	153,892.25	141,331.83
		141,331.83=4×400+133,663.08×0.7+153,892.25×0.3		
Hybrid robust	3,25,51,104	142,595.36	157,057.39	148,533.97
		148,533.97=4×400+142,595.36×0.7+157,057.39×0.3		
Robust model	3,25,51,104	0	157,057.39	158,657.39
		158,657.39=4×400+157,057.39×1		

As shown in Table VIII, the optimal line hardening strategy is {25, 51, 65, 104} based on the proposed ART-DAD model, and the total expected costs for attacks are 265,457.68$. Notably, the solution time on this larger IEEE RTS-96 system is 51.17 minutes and still within one hour time frame. This implies that the proposed ART-DAD model can be effectively solved by the constraint-generation based solution algorithm for the large-scale power system. The operation cost follows the similar trend as of the previous case studies in the IEEE RTS-79 system. In addition, Table IX compares the simulation results between the proposed ART-DAD model and two other models including the hybrid robust and robust defense models. The total expected costs are minimized by the proposed ART-DAD model. This fact indicates that the proposed method is effective against uncertain attacks in power systems with high wind power penetration, compared to the conventional approaches.

Case 7: In this case study, the proposed ART-DAD model is tested from the cost perspective under different defense resources and attack budget probabilities.

As shown in Fig. 4, the attack budget scenarios set is ***S***= (2, 3). The total expected costs decrease following the attack budget probabilities when 2 attacked lines (R_A=2) outweighs the probability of 3 attacked lines (R_A=3). However, when the defense resource R_L is within a certain range, the total expected costs may remain unchanged due to the marginal cost of hardening line. To investigate the impact of the marginal cost of hardening line, Π is set at 0.5, and Table X shows defense strategies under different marginal costs of hardening line (i.e., 400$/meter and 800$/meter). It can be found that the different marginal costs of hardening line may also impact the decisions of defended lines. Notably, the total number of actual hardened lines may not always vary with the defense resource R_L. For example, when the marginal cost of hardening line is set to 800$/meter, if the defense resource is greater than 7 lines, total number of hardened lines will remain to be 7 without further increase. This is because it may de-motivate the system operator to further harden much more lines due to the high marginal cost of hardening lines. In addition, the marginal cost of hardening line is much higher than the marginal cost of the system operation, which offsets the benefit of line hardening strategy to reduce the total expected costs. These results mean that the proposed ART-DAD model is helpful for the system operator to make a more objective assessment of the defense resources, in order to formulate a reasonable defense strategy by considering the marginal costs and benefits of hardening lines.

TABLE X

DEFENSE STRATEGIES UNDER DIFFERENT DEFENSE RESOURCES AND MARGINAL COST OF HARDENING LINE ON THE IEEE RTS-96 SYSTEM

R_L	Line hardening cost 400$/meter	Line hardening cost 800$/meter
4	3,39,51,118	1,38,51,118
5	3,39,51,118	3,39,51,118
6	1,38,51,61,118	3,39,51,110
7	3,20,39,51,61,104,118	1,25,39,51,61,100,117
8	3,20,31,51,61,71,104,110	1,25,38,51,61,100,110

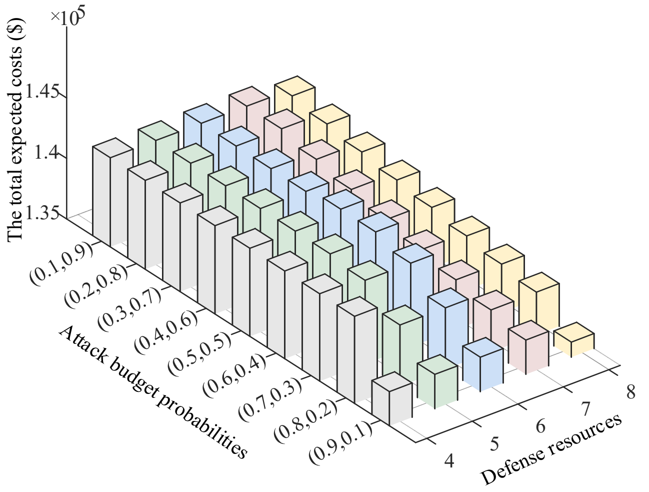


Fig. 4. Total expected costs on the IEEE RTS-96 system in different attack and defense scenarios.

V. Conclusion

In this paper, we present an adjustable robust tri-level defender-attacker-defender (ART-DAD) model against both uncertainties from power system attacks and high wind power penetration. The constraint-generation based solution algorithm is employed to solve the proposed ART-DAD model with a master and sub-problem scheme. Extensive case studies verify that the proposed defense model can effectively mitigate the impacts of uncertain attacks and improve the resilience of power systems compared to traditional defense models. The ART-DAD model developed in this paper can provide a practical method to handle power system uncertainties including the attack uncertainty and wind power output uncertainty. In practice, by properly setting the level of conservatism in the uncertainty set, the proposed model can optimize the total expected costs of system operation and adopt new line defense strategies with various attack budget scenarios and defense resources. In the future work, we will conduct further research focusing on how to improve the power system resilience against attacks in the presence of multiple uncertainties. In addition, we will extend the proposed approach to protect other network components to further improve the resilience of power systems.

Acknowledgement

This work was supported in part by the UK Research and Innovation Future Leaders Fellowship entitled 'Digitalisation of Electrical Power and Energy Systems Operation' under Grant MR/W011360/2.

Appendix

A. Framework of constraint-generation based solution algorithm

The master and sub-problem are formulated as a compact form and iteratively solved by the following constraint-generation based solution algorithm framework. In the algorithm 1solution steps, the master problem is formulated as equations (46-49), where (46) represents (18), (47) represents (19), (48) represents (20), (49) represents (21)-(28) as a compact form of each equation. The sub-problem is formulated as equations (50-52), where (50) represents (37), (51) represents (38), (52) represents (39)-(44) as a compact form of each equation. Fig. 5 shows the flowchart of the constraint-generation based algorithm. In this paper, the optimality tolerance ε is set at 0.01 to complete iterations for an optimal solution.

Algorithm 1: Master and Sub-Problem Solution

Initialization: $\bar{L} \leftarrow -\infty$, $\bar{U} \leftarrow +\infty$, $\hat{\boldsymbol{A}} \leftarrow (\mathbf{1}, \bar{\boldsymbol{W}})$, $m \leftarrow 1$, $\varepsilon \leftarrow +\infty$, and $ns \leftarrow 1$. Here, $\bar{\boldsymbol{W}}$ is the predicted wind power output.

1. Master problem:

① Based on $\hat{\boldsymbol{A}}$, solve the master problem:

$$\rho = \min_{\boldsymbol{d},\omega} \boldsymbol{c}^{\mathrm{T}}\boldsymbol{d} + \omega \tag{46}$$

subject to:

$$\boldsymbol{L}^{\mathrm{T}}\boldsymbol{d} \le \boldsymbol{b} \tag{47}$$

$$\omega \ge \sum_{s\in \boldsymbol{S}} [\Omega(s)\boldsymbol{P}^{\mathrm{T}}\boldsymbol{y}_k(s))] \qquad k = 1,...,m \tag{48}$$

$$\boldsymbol{I}^{\mathrm{T}}\boldsymbol{d} + \boldsymbol{J}^{\mathrm{T}}\hat{\boldsymbol{a}}_k(s) + \boldsymbol{U}^{\mathrm{T}}\hat{\boldsymbol{w}}_k(s) + \boldsymbol{R}^{\mathrm{T}}\boldsymbol{y}_k(s) \le \boldsymbol{e} \quad k = 1,...,m \tag{49}$$

Record the best feasible solution $(\hat{\boldsymbol{d}}, \hat{\omega}, \hat{\rho})$ found in the k-th iteration.

② Update $\bar{L} \leftarrow \hat{\rho}$ and $m \leftarrow m+1$.

2. Sub-problem:

① Given $\hat{\boldsymbol{d}}$, solve the dual subproblem:

$$Q(s) = \max_{\boldsymbol{a}(s),\boldsymbol{\pi}(s),\boldsymbol{w}(s)} \boldsymbol{C}^{\mathrm{T}}\boldsymbol{\pi}(s) + \boldsymbol{D}^{\mathrm{T}}\boldsymbol{w}(s) \tag{50}$$

subject to:

$$\boldsymbol{B}^{\mathrm{T}}\boldsymbol{a}(s) + \boldsymbol{Y}^{\mathrm{T}}\boldsymbol{w}(s) \le \boldsymbol{h} \tag{51}$$

$$\boldsymbol{H}^{\mathrm{T}}\hat{\boldsymbol{x}} + \boldsymbol{E}^{\mathrm{T}}\boldsymbol{a}(s) + \boldsymbol{F}^{\mathrm{T}}\boldsymbol{\pi}(s) \le \boldsymbol{t} \tag{52}$$

Record the best feasible solution $(\hat{Q}_m(s), \hat{\boldsymbol{a}}_m(s), \hat{\boldsymbol{w}}_m(s), \hat{\boldsymbol{\pi}}_m(s))$ found in the m-th iteration.

② Update $\hat{\boldsymbol{A}} = \hat{\boldsymbol{A}} \cup (\hat{\boldsymbol{a}}_m(s), \hat{\boldsymbol{w}}_m(s))$ and $ns \leftarrow ns+1$ until all possible attack budget scenarios are considered (i.e., $ns > Ns$), otherwise repeat sub-step ① and ②.

③ Set $\bar{U} \leftarrow \min\{\bar{U}, (\hat{\rho} - \hat{\omega}) + \sum_{s\in \boldsymbol{S}} [\Omega(s)\hat{Q}_m(s)]\}$.

3. Optimality test:

① Set $\varepsilon = \min\{\varepsilon, (\bar{U} - \bar{L}) / \bar{L}\}$, and determine whether ε is less than or equal to 0.01, i.e., $\varepsilon \le 0.01$?

② **Exploitation:** If $\varepsilon \le 0.01$, then terminate and output the optimal decisions.

Exploration: If $\varepsilon > 0.01$, and go back to step 1.

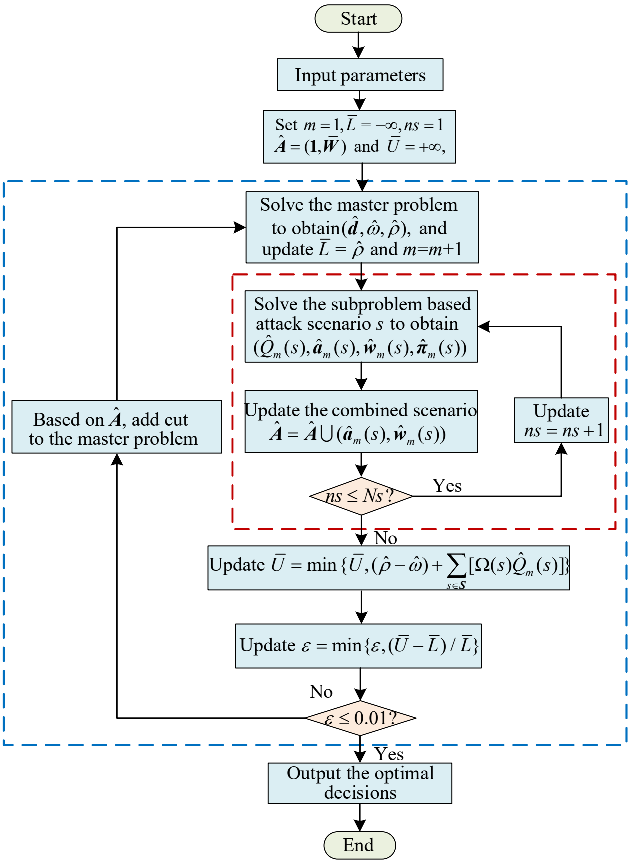


Fig. 5. Flowchart of the constraint-generation based solution algorithm.

REFERENCES

[1] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Power Systems Resilience Assessment: Hardening and Smart Operational Enhancement Strategies," *Proceedings of the IEEE,* vol. 105, no. 7, pp. 1202-1213, 2017.

[2] B. Yan, Z. Jiang, P. Yao, Q. Yang, W. Li, and A. Y. Zomaya, "Game Theory Based Optimal Defensive Resources Allocation with Incomplete Information in Cyber-Physical Power Systems Against False Data Injection Attacks," *Protection and Control of Modern Power Systems,* vol. 9, no. 2, pp. 115-127, 2024.

[3] M. Liu *et al.*, "Enhancing Cyber-Resiliency of DER-Based Smart Grid: A Survey," *IEEE Transactions on Smart Grid,* pp. 1-1, 2024.

[4] C. Qin, C. Zhong, B. Sun, X. Jin, and Y. Zeng, "A tri-level optimal defense method against coordinated cyber-physical attacks considering full substation topology," *Applied Energy,* vol. 339, p. 120961, 2023/06/01/ 2023.

[5] M. Kamal, M. Farajollahi, H. Nazaripouya, and H. Mohsenian-Rad, "Cyberattacks Against Event-Based Analysis in Micro-PMUs: Attack Models and Counter Measures," *IEEE Transactions on Smart Grid,* vol. 12, no. 2, pp. 1577-1588, 2021.

[6] T. Ding, Y. Lin, Z. Bie, and C. Chen, "A resilient microgrid formation strategy for load restoration considering master-slave distributed generators and topology reconfiguration," *Applied Energy,* vol. 199, pp. 205-216, 2017/08/01/ 2017.

[7] "ABC NEWs, Powerful storm pounds the Black Sea region, leaving more than a half-million people without power" November 2023, [Online]."Available:https://abcnews.go.com/International/wireStory/half-million-people-left-power-crimea-after-black-105174488."."

[8] Z. Liu and L. Wang, "A Distributionally Robust Scheme for Critical Component Identification to Bolster Cyber-Physical Resilience of Power Systems," *IEEE Transactions on Smart Grid,* vol. 13, no. 3, pp. 2344-2356, 2022.

[9] Z. Bie, Y. Lin, G. Li, and F. Li, "Battling the Extreme: A Study on the Power System Resilience," *Proceedings of the IEEE,* vol. 105, no. 7, pp. 1253-1266, 2017.

[10] J. M. Arroyo and F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem," *IEEE Transactions on Power Systems,* vol. 20, no. 2, pp. 789-797, 2005.

[11] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez, "Trilevel Optimization in Power Network Defense," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews),* vol. 37, no. 4, pp. 712-718, 2007.

[12] W. Yuan, L. Zhao, and B. Zeng, "Optimal power grid protection through a defender–attacker–defender model," *Reliability Engineering & System Safety,* vol. 121, pp. 83-89, 2014/01/01/ 2014.

[13] T. Xu, C. Shao, M. Shahidehpour, and X. Wang, "Coordinated Planning Strategies of Power Systems and Energy Transportation Networks for Resilience Enhancement," *IEEE Transactions on Sustainable Energy,* pp. 1-12, 2022.

[14] Z. Liu and L. Wang, "Leveraging Network Topology Optimization to Strengthen Power Grid Resilience Against Cyber-Physical Attacks," *IEEE Transactions on Smart Grid,* vol. 12, no. 2, pp. 1552-1564, 2021.

[15] "Current Energy Production." Jul. 2021. [Online]. Available: https://en.winddenmark.dk/wind-in-denmark/statistics/wind-amount."

[16] S. Zhao, Q. Yang, P. Cheng, R. Deng, and J. Xia, "Adaptive Resilient Control for Variable-Speed Wind Turbines Against False Data Injection Attacks," *IEEE Transactions on Sustainable Energy,* vol. 13, no. 2, pp. 971-985, 2022.

[17] S. Zhao, J. Xia, R. Deng, P. Cheng, Q. Yang, and X. Jiao, "Dual-Triggered Adaptive Torque Control Strategy for Variable-Speed Wind Turbine Against Denial-of-Service Attacks," *IEEE Transactions on Smart Grid,* vol. 14, no. 4, pp. 3072-3084, 2023.

[18] S. Zhao, J. Xia, R. Deng, P. Cheng, and Q. Yang, "Adaptive Observer-Based Resilient Control Strategy for Wind Turbines Against Time-Delay Attacks on Rotor Speed Sensor Measurement," *IEEE Transactions on Sustainable Energy,* vol. 14, no. 3, pp. 1807-1821, 2023.

[19] A. Bagheri, C. Zhao, F. Qiu, and J. Wang, "Resilient Transmission Hardening Planning in a High Renewable Penetration Era," *IEEE Transactions on Power Systems,* vol. 34, no. 2, pp. 873-882, 2019.

[20] X. Wang, Z. Li, M. Shahidehpour, and C. Jiang, "Robust Line Hardening Strategies for Improving the Resilience of Distribution Systems With Variable Renewable Resources," *IEEE Transactions on Sustainable Energy,* vol. 10, no. 1, pp. 386-395, 2019.

[21] Z. Liu and L. Wang, "A Distributionally Robust Defender-Attacker-Defender Model for Resilience Enhancement of Power Systems Against Malicious Cyberattacks," *IEEE Transactions on Power Systems,* vol. 38, no. 6, pp. 4986-4997, 2023.

[22] A. Zhou, M. Yang, T. Wu, and L. Yang, "Distributionally Robust Energy Management for Islanded Microgrids With Variable Moment Information: An MISOCP Approach," *IEEE Transactions on Smart Grid,* vol. 14, no. 5, pp. 3668-3680, 2023.

[23] Y. Xiang and L. Wang, "An Improved Defender–Attacker–Defender Model for Transmission Line Defense Considering Offensive Resource Uncertainties," *IEEE Transactions on Smart Grid,* vol. 10, no. 3, pp. 2534-2546, 2019.

[24] Y. Xiang, X. Zhang, D. Shi, R. Diao, and Z. Wang, "Robust optimization for transmission defense against multi-period attacks with uncertainties," *International Journal of Electrical Power & Energy Systems,* vol. 121, p. 106154, 2020.

[25] M. Du, X. Liu, Q. Zhou, and Z. Li, "Hybrid Robust Tri-Level Defense Model Against Multiperiod Uncertain Attacks," *IEEE Transactions on Smart Grid,* vol. 13, no. 4, pp. 3255-3265, 2022.

[26] A. Attarha, N. Amjady, and A. J. Conejo, "Adaptive robust AC optimal power flow considering load and wind power uncertainties," *International Journal of Electrical Power & Energy Systems,* vol. 96, pp. 132-142, 2018.

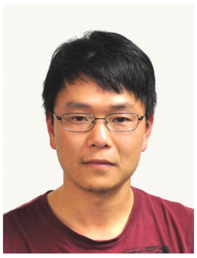
[27] F. Verástegui, A. Lorca, D. E. Olivares, M. Negrete-Pincetic, and P. Gazmuri, "An adaptive robust optimization model for power systems planning with operational uncertainty," *IEEE Transactions on Power Systems,* vol. 34, no. 6, pp. 4606-4616, 2019.

[28] C. Grigg, "The IEEE reliability test system 1996," *Proc. IEEE PES Winter Power Meeting,* pp. 1010-1020, 01/01 1996.

[29] H. Ye, J. Wang, Y. Ge, J. Li, and Z. Li, "Robust Integration of High-Level Dispatchable Renewables in Power System Operation," *IEEE Transactions on Sustainable Energy,* vol. 8, no. 2, pp. 826-835, 2017.

Min Du (Member, IEEE) received the B.Sc. degree from the School of Electrical and Information Engineering, Wuhan Institute of Technology, Wuhan, China, in 2016, and the M.Sc. and Ph.D. degrees from the College of Electrical and Information Engineering, Hunan University, Changsha, China, in 2019 and 2023, respectively. He is currently a Postdoctoral Research Associate with The University of Sheffield, U.K. His research interests include cyber-physical power systems, cybersecurity, and resilience.

Jinning Zhang received the B.S. in vehicle engineering from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2018 and received the M.Sc. and Ph.D. degree in Aerospace Propulsion with Cranfield University, U.K in 2019 and 2022. She is currently a Lecturer (Assistant Professor) in Aerospace and Computational Engineering with University of Leicester, UK. Her research interests include energy management strategies and integrated control system design for aerospace propulsion, AI for transport and energy systems, and transportation-energy nexus.



Chenghong Gu (Member, IEEE) received the Ph.D. degree from the University of Bath, Bath, U.K. He is a Reader with the Department of Electronic and Electrical Engineering, University of Bath, UK. Previously, he was an EPSRC Research Fellow with the University of Bath. His major research interest is in energy system resilience, multi-vector energy systems, and power economics and markets. Dr Gu is the Co-Editor-in-Chief for IET Smart Grid and Associate Editor for IEEE Transactions on Power Systems

Xin Zhang (Senior Member, IEEE) received the B.Eng. degree in automation and control systems from Shandong University, China, in 2007, the M.Sc. and Ph.D. degrees in electrical power engineering from The University of Manchester, U.K., in 2007 and 2010, respectively. He is currently a Professor of Control and Power Systems with The University of Sheffield, U.K. From 2022, he was awarded the U.K. Research and Innovation (UKRI) Future Leaders Fellowship, and U.K. Engineering and Physical Sciences Research Council (EPSRC) New Investigator Award. From 2021 to 2023, he was an Associate Professor with Brunel University London, U.K. From 2019 to 2021, he was a Senior Lecturer with Cranfield University, U.K. From 2011 to 2019, He was with National Grid Electricity System Operator, Wokingham, U.K. His research interests include power system control and operation, cyber-physical power systems modelling and co-simulation, and grid-integrated transport electrification.